Additional Questions for the Record

Manny Cancel, Chief Executive Officer, Electricity Information Sharing and Analysis Center

The Honorable Richard Hudson

1a. How can redundancy in grid transmission lead to grid resilience?

Transmission redundancy provides for additional, alternate electrical paths from energy supply to load, or completely separate electrical paths from load to diverse supplies of electrical energy. These supplies can be nearby the load, or long distance depending on energy availability and/or deficiencies. Transmission planning seeks to ensure that flows on a networked transmission system remain within system and interconnection operating limits for a range of events and contingencies. In addition to enabling recovery and reducing the duration of extreme event transmission outages, circuit redundancy furthers grid resilience by providing means to anticipate, plan, withstand, adapt to, and protect against extreme events on the transmission system.

1b. What is Congress's role in improving or increasing transmission?

It is critically important that lawmakers and policymakers understand the central role that transmission development plays in the energy transition — not only to support the evolving electricity resource mix, but also the electrification of infrastructures. New electric generation developments, primarily wind and solar, are typically located where the resources will produce optimally, requiring new transmission to deliver their power to load centers and reliably handle new electricity flow patterns. Further, as solar and wind generating output is variable more transmission is needed to create options for operators by providing energy flows from areas that have energy available, to support those areas that are deficient due to the loss of fuel sources. Earlier this year, Congress directed NERC to conduct a study on interregional transfer capability. The analysis of interregional transfer capability from a reliability perspective will play an important part of overall transmission planning.

Adoption rates for electric vehicles and electrification programs have the potential to significantly alter not only peak demand, but also hourly demand patterns. This can alter the needed capacity for the transmission system and complicates transmission planning with considerations for all-hour energy flows.

A key factor underlying the energy transition is the time it takes time to build high-voltage transmission, and the extraordinary siting challenges that can be encountered. In recent years, transmission development in many regions has stalled and many transmission planning entities report significant permitting and siting issues causing delays. This is especially true of interstate and inter-market transmission which can support the evolving resource mix and electric demand growth. Policies aimed at electrification and energy transition must account for the current realities of transmission development, as stakeholders address obstacles with permitting and siting. Congress can help in this area by continuing to pursue improvements to the permitting process for transmission and other energy infrastructure.

1c. Please provide insight on both regional transmission and interregional transmission.

The continental U.S. transmission system is comprised of three interconnections with limited DC connections between them: the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas. Further, there are AC transmission links to most bordering Canadian provinces, through DC ties with the Québec interconnection. Each US interconnection

contains one or more of the twelve transmission planning regions established pursuant to FERC Order 1000 (2011). Among other things, FERC Order 1000 requires that each public utility transmission provider participate in a regional transmission planning process. Order 1000 also seeks to improve coordination between neighboring transmission planning regions for new interregional transmission facilities.

As the grid transforms, comprehensive transmission planning supported by robust interregional coordination is essential for reliability and resilience. Regional planning seeks to ensure that the local plans of individual transmission owners/operators are coordinated with their interconnected and similarly situated neighboring transmission systems so that the reliability, public policy and economic needs within the planning region are optimally met. Interregional transmission planning focuses on identifying and developing transmission projects that provide benefits across two or more planning regions. As stated in a recent DOE report, "regional grid reliability is strengthened by the diversity of generation provided by interregional transfers, regions need to import electricity when they cannot meet growing demand with local generation or when the combination of remote generation and interregional transmission has lower overall system costs than local generation, or a combination of these."[1] In addition, transmission will be

[1] National Transmission Needs Study - Draft for Public Comment (February 2023) (energy.gov)

critical to address the growth in regional generating uncertainty from the increase in energy-constrained resources that depend on weather conditions.

Regional, and, more importantly, interregional transmission can play a significant role in effectively adding fuel supply diversity to a generation fleet that is increasingly dependent upon just in time fuel sources (e.g., natural-gas, wind, and solar). Transporting various fuel types from areas of relative fuel abundance to areas experiencing fuel supply interruptions is often challenging, and, in some cases, impossible when generation resources are located far from loads and transmission is limited. However, electrical energy can instantly be transmitted many hundreds of miles to areas where local fuel unavailability issues might arise, particularly during extreme weather events.

The role of interregional transmission in supporting energy adequacy through fuel supply diversity is an area in need of further independent assessment. The Interregional Transfer Capability Study (ITCS) that Congress directed NERC to perform is an important opportunity to analyze this topic from a reliability perspective, providing important information related to transmission and the ability to incorporate this analysis more directly into future reliability assessments.

2. Are there any updates needed to the Cybersecurity Risk Information Sharing Program? What is Congress's role in facilitating those updates?

The Cybersecurity Risk Information Sharing Program (CRISP) is a unique public-private capability that provides actionable threat actor information in near real time to help utilities defend themselves. As adversaries increase capabilities and evolve tactics, CRISP must continue to evolve from a technology and capability perspective. Ensuring CRISP maintains its connection to the Intelligence Community, and near-real-time sharing of information of participating utility data, are essential to success. Working closely with DOE's Offices of Cybersecurity and Energy Security, Science, and Intelligence, NERC, as the program steward, is committed to ensuring CRISP's long-term future, capability, and success.

Additional support to grow technology capabilities, including capital and personnel expenditures, will help the program to adjust to new threats and increased scale of data sharing. There is a cost to participating in the program, and funding opportunities such as the 2021 Infrastructure Act would enable further expansion

and lowering of participant costs. Examples of funding opportunities include expansion of membership, increased data analysis, and the ability to better monitor for and report on malicious activity.

3. How is E-ISAC ensuring their specific and actionable workshops are providing utilities with mitigation strategies, while also ensuring bad actors are unable to attend?

The Electricity Information Sharing and Analysis Center (E-ISAC) is a membership-based information sharing community focused on reducing cyber and physical risk to the electricity industry across North America. The E-ISAC community is comprised of a trusted network of electricity asset owners and operator members and select government and cross-sector partners. Being a part of the E-ISAC community is voluntary, and all member organizations are vetted in accordance with the E-ISAC's Account Management Policy and in accordance with federal government guidelines intended to limit participation by nation state actors. Each E-ISAC member is also vetted by their organization's Designated Approving Official (DAO), a trusted point of contact at each organization responsible for validating each of their organization's Portal users' roles and need for access to the secure E-ISAC Portal. Together, the E-ISAC community comes together to exchange critical information and actively engage in programs, exercises, conferences, and workshops in support of a strong, secure, and resilient bulk power system.

In response to threats to the electricity industry, the E-ISAC develops products and services to help inform E-ISAC members of the threats, shares mitigation strategies, and remains available for member support. From workshops, conferences, and webinars, to reports, bulletins, and white papers, the E-ISAC uses various formats to communicate with its members. Below is a description of some of the workshops and other products the E-ISAC offers to its members.

VISA Workshop

In 2015, the Electricity Information Sharing and Analysis Center's Physical Security Advisory Group (PSAG) developed the Design Basis Threat (DBT) reference document to assist asset owners and operators (AOO) in assessing the security of bulk power system physical infrastructure. A DBT is defined as the threat against which an asset must be protected and upon which the protective system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The DBT

includes the tactics aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics.

The DBT is taught through the Vulnerability of Integrated Security Analysis (VISA) workshop. This workshop educates vulnerability assessment practitioners on the process to implement a DBT. Each workshop is tailored to the particular host organization. A scenario is created and implemented to assess acceptable consequences and develop upgrades and protective measures to protect against those scenarios. The E-ISAC has facilitated over 17 workshops to date. The vast majority have led the member to making specific upgrades and additional protective measures to defend their facility.

For each VISA workshop, the E-ISAC works directly with the utility to determine appropriate participation from members of the organization and local law enforcement. The host utility reviews each registration. The E-ISAC, facilitators, and any outside law enforcement entities are required to sign a non-disclosure agreement about the information provided during the workshop. Because the workshop is scenario-based, working off the utilities' actual facilities, the information would be damaging if it became public; therefore, all information from the scenarios are destroyed after the workshop.

CRISP Workshop

CRISP hosts a biannual spring and fall workshop for the CRISP community. Each workshop is typically two to three days. The purpose of the workshops is to update CRISP members on the program, provide classified and unclassified briefings on current topics, trends, and areas of concern, and provide hands on trainings to continue to advance the capabilities of members' staff. Since 2022, the E-ISAC has expanded the invitation for attendance to trade organizations, Canadian partners, and non-CRISP members to better engage and support the energy sector. These non-CRISP members are able to join all facets of the workshop (excluding the program update) thereby expanding the workshop to the energy sector in general.

Monthly Briefing

The Monthly Briefing is a webinar-based briefing designed to cover timely security topics within the electricity industry. The Monthly Briefing is reserved for E-ISAC members, including energy asset owners, operators and their representatives, vetted staff from cross-sector ISACs who maintain active E-ISAC Portal accounts, and occasionally invited energy sector partners and guests. The content generally includes an overview of the current threat landscape and mitigation recommendations.

GridSecCon

GridSecCon is the E-ISAC's annual conference that brings together cyber and physical security leaders from industry and government to deliver expert training sessions, share best practices and effective threat mitigation programs, and present lessons learned. Attendees participate in a full day of training, two days of keynote presentations and panels, breakout sessions focused on cyber and physical security issues impacting the industry, and a day of threat briefings and security-focused tours. GridSecCon attendees benefit from both the educational aspect of the conference and networking opportunities.

GridEx

Every two years, the E-ISAC hosts GridEx, the largest grid security exercise in North America. GridEx consists of two components: Distributed Play, a two-day operational exercise developed primarily for E-ISAC Members and Partners, and the Executive Tabletop, a one-day, policy-focused, invitation-only event. Distributed Play is a decentralized operational exercise focused on response and recovery. The Executive Tabletop convenes key industry and government leaders to examine the extraordinary measures needed to respond to severe cyber and physical attacks at a policy and strategic level, and to coordinate executive and national level decision-making in a more geographically focused scenario.

GridEx Distributed Play provides a common forum, coordinated across all participating E-ISAC members and partners, to practice response to and recovery from a coordinated cyber and physical security threat. The Executive Tabletop has resulted in key developments and services for industry, such as the Cyber Mutual Assistance program, which is managed by the Edison Electric Institute.

4. How do you recommend shaping market forces to drive security and resilience? Specifically, please consider distribution transformers.

As the ERO, NERC is not directly involved in the functions or design of wholesale electricity markets, or the markets for equipment, support, or commodities used in the planning and operation of the BPS. However, NERC performs a critical function in monitoring and assessing the reliability and security of the BPS. This often involves considering the effects of market mechanisms, as well as government policies and grid planning processes, in meeting the reliability and security needs of BPS owners and operators. NERC's Long-Term Reliability Assessments identify issues facing the current and future system adequacy and resilience of the BPS through systematic assessment of forecasted demand and resources, transmission system projections, and emerging risks arising from various market, policy, technological, or economic

factors.[2] Recent LTRAs have warned of the risk of energy supply shortfalls stemming from disorderly retirement of generators and the resulting impacts to resource adequacy and fuel supply sufficiency, the potential impact of inadequate performance standards and capabilities in our growing inverter-based resource fleet, and the need for transmission investment to support the resource mix transition and extreme weather resilience.

In NERC's recent seasonal reliability assessments, published ahead of each winter and summer peak periods, NERC recognized that many U.S. electric utilities are reporting low inventories of distribution transformers.[3] This has the potential to challenge efforts to restore the distribution system following severe summer and winter weather. Weather events such as hurricanes, tornadoes, and ice storms can cause significant damage to distribution power lines, poles, and transformers. Insufficient supplies of distribution transformers can delay and complicate the critical field operations of restoring electrical service to customers.

Addressing the risks to security and resilience as the grid rapidly transforms requires concerted effort from the broad electricity stakeholder community. In the 2022 LTRA, NERC advised that reliability must be a top priority for the community of stakeholders involved in resource and system planning in order to reduce the potential for energy policies and market designs to have unintended consequences on the BPS. Market designers, monitors and regulators that oversee market performance play an important role in ensuring reliability and resilience. Wholesale electricity markets may not inherently value reliability and resilience attributes, making it necessary for mechanisms to be designed that will, (i) provide sufficient incentives for owners and operators to invest in their equipment or service to ensure security, reliability, and resilience, (ii) adequately compensate owners and operators for the costs of providing important services, such as firm fuel to generators, or, (iii) adequately reflect the potential costs of disruption to reliable and secure BPS performance, such as lost economic activity or damages to the BPS. Regulators and policymakers also need to consider how policies will affect markets and supply chains for BPS equipment and services needed for a reliable, resilient, and secure grid. With a critical need for distribution

[2] Access NERC's LTRAs and other reliability assessments at the NERC webpage: https://www.nerc.com/pa/RAPA/ra/Pages/default.aspx

[3] See NERC's 2023 Summer Reliability Assessment, pp 6-7: https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2023.pdf

transformers already affected by complex supply chains for skilled labor and specialized steel, NERC is aware of concerns regarding proposed distribution transformer efficiency standards and the impact on transformer availability.

In the security arena, NERC's Critical Infrastructure Protection standards (CIP) provide a baseline for essential security practices. Upon direction by Congress, the Federal Energy Regulatory Commission recently promulgated market rules that provide additional return on security investments that go above and beyond those required by CIP. Given the increased risk from supply chain cyber and physical security threats, NERC and the E-ISAC are working with equipment manufacturers to share threat information rapidly. Through the E-ISAC Vendor Affiliate Program, utilities and manufacturers discuss at a high level how to harmonize incident reporting to critical infrastructure customers to help operators better understand the risk from supply chain compromises, and the mitigations.